Click here to view PowerPoint presentation; Press Esc to exit

NATO Military Messaging in the Tactical Domain – Performance Issues of an HF Channel

Vivianne Jodalen, Anders Eggen, Bjørn Solberg and Ove Grønnerud
Norwegian Defence Research Establishment (FFI)
P.O. Box 25
N-2027 Kjeller
NORWAY

E-mail: vjo@ffi.no, ane@ffi.no, bso@ffi.no, okg@ffi.no

SUMMARY

NATO STANAG 4406 for Military Message Handling Systems (MMHS) may be used for direct information exchange between the high data rate strategic domain and the low data rate tactical domain by using the tactical protocol profile specified in Annex E. This paper explores the performance of the MMHS application over NATO standardized HF radio systems using both unicast and multicast IP services. A comparison of performance is made with a dedicated HF messaging application, and advantages/disadvantages by using the IP based application are pointed out. MMHS Annex E over HF systems is a viable solution, providing application throughputs up to a few kilobits per second. There are however, optimisation issues at different levels of the protocol stack, and we have seen that implementation choices and parameter settings have great impact on the overall performance of the system.

1.0 INTRODUCTION

Interoperability between communications equipment used by military forces from different countries is very important in todays battlefields. During the last ten years NATO has produced a number of standards (STANAGs) for military information systems, ranging from applications to bearer services such as HF communications. Using standardized protocols at all levels of the protocol stack provides interoperability and flexibility. IP will be the integrating networking technology in future military communications network, and many nations are planning to use IP as a platform for their communication systems in both the strategic and tactical domains. This will provide increased interoperability between strategic and tactical systems. However, there may be challenges when the TCP/IP protocol suite is used over tactical communication systems with variable quality and data rate. Traditionally for tactical communication systems, applications have been uniquely tailored to the bearer service. This provides efficient utilization of the channel capacity, but at the cost of flexibility and re-use of the same applications.

This paper describes the exploration in the lab and over-the-air of a NATO standardized application; the Military Message Handling System (MMHS) specified in STANAG 4406, used together with NATO standardized HF communication systems specified in STANAG 4538 (3G HF) and STANAG 5066 (2G HF). A new HF datalink protocol (HDL+) proposed for standardisation, is also included in the evaluation. STANAG 4406 for MMHS includes both a strategic and a tactical protocol profile, which may be used for exchanging information between the high data rate strategic domains and the low data rate tactical domain. We discuss the use of IP as an integrator between the MMHS application and the HF bearer services. The MMHS may also be used as an integrator between tactical bearer systems such as HF/VHF/UHF/WLAN.

Jodalen, V.; Eggen, A.; Solberg, B.; Grønnerud, O. (2006) NATO Military Messaging in the Tactical Domain – Performance Issues of an HF Channel. In *Military Communications* (pp. 11-1 – 11-16). Meeting Proceedings RTO-MP-IST-054, Paper 11. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
NATO Military Messaging in the Tactical Domain Performance Issues of an HF Channel	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Norwegian Defence Research Establishment (FFI) P.O. Box 25 N-2027 Kjeller NORWAY**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**56**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

In NATO Network Enabled Capabilities (NNEC) seamless interconnection of systems and networks is an important factor. In the migration process towards NNEC, we believe the MMHS based on STANAG 4406 may be used as an integrator between strategic and tactical systems because most NATO nations (including the NATO organization) recently have procured systems in accordance with this standard.

2.0 NATO MILITARY MESSAGING

A Formal Military Message is different from an interpersonal message in that it is a message sent on behalf of an organization, and that it establishes a legal commitment on the sending and receiving organization under military law. Examples of formal messages are military orders.

Formal Military Messages are handled by Military Message Handling Systems (MMHSs). An MMHS takes responsibility for the delivery, formal audit, archiving, numbering, release, emission, security and distribution of received formal messages. In NATO, the formal messaging service is seen as the vehicle for secure, mission critical, operational, military applications (e-mail systems are not). STANAG 4406 Ed.1[1] [1] is the only agreed standard to achieve interoperability between the formal messaging systems of NATO nations. Systems compatible with the S4406 standard have been and are being implemented widely by the NATO nations and by the NATO organization.

2.1 Military Messaging in the tactical domain

The original connection oriented protocol stack defined in S4406 Annex C (and ACP 123 [2]) was developed for strategic high data rate networks, and is not suitable for channels with low data rate. A protocol solution defined in Annex E of S4406 has therefore been developed for *tactical* communications. With the inclusion of this protocol profile in S4406, a common baseline protocol solution exists that opens for a seamless interconnection of MMHS between the strategic (fixed) and tactical (mobile) environments. One messaging system may therefore be used to communicate with all national forces, the NATO organization and the NATO allies. In Figure 1 the MTA (Message Transfer Agent) may be used as a gateway between the strategic and tactical domain if the dual stack is implemented.

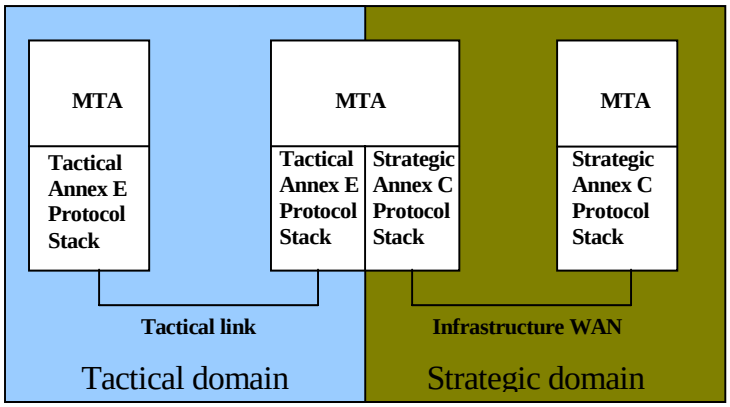


Figure 1: Seamless interconnection of MMHS between the strategic and tactical domain

To take account of the characteristics of a tactical radio link, the Annex E protocol profile has adopted the following:

[1] STANAG 4406 Edition 2 is out for NATO ratification at the time of writing.

- A connectionless protocol stack, which gives less overhead and reduces the effect of large turn-around times of the link
- A choice of full-duplex, half-duplex or simplex (broadcast) operation
- Compression to reduce the amount of data transmitted
- It may be used for both Unicast and Multicast, the latter providing efficient use of radio resources
- Procedures for handling EMCON recipients

The protocol profile in Annex E is divided into an application layer and a transport layer on top of potential bearer systems. Among several sub-layers, the P-Mul protocol (ACP-142 [3]) is introduced to compensate for the lack of transfer reliability of the connectionless protocol stack. It splits the message into smaller Protocol Data Units (PDU's), attaches a checksum, numbers the PDU's and handles retransmissions based on a selective repeat procedure. The P-Mul sub-layer has also functionality for both multicasting and unicasting of messages. The transport layer of Annex E uses a connectionless WAP protocol called the Wireless Datagram Protocol (WDP). This protocol is more flexible than the UDP protocol in that it does not mandate the use of IP. However, for IP networks the WDP protocol becomes UDP. In our test where the HF radio provides an IP service, Annex E uses the UDP protocol.

These features of Annex E increase the messaging throughput substantially for tactical communication channels with low data rate compared to the connection oriented Annex C protocols. We have used the Thales XOmail implementation of S4406 in our tests, including both the tactical (Annex E) and strategical (Annex C) protocol profiles.

3.0 TACTICAL RADIO COMMUNICATIONS

Tactical communications are used by highly mobile units not being able to utilize a fixed communications infrastructure. Typical tactical units requiring long range tactical communications are: Naval vessels, aircrafts, land mobiles and special forces carrying manpack radios. The characteristics of long range tactical radio communications in general are:

- Only low to moderate data rate is supported (typically < 10 kbit/s)
- Variable data rate depending on time, location and other users of the radio spectrum
- Unreliable connections; high bit error rates, frequent link terminations, unreachable nodes, equipment failure
- Half duplex or simplex channels, giving large turn-around times
- Different types of radio equipment
- Emission Control (radio silence) conditions are often required

3.1 NATO HF Communications

The above characteristics apply to HF communications in particular, since HF propagates via reflecting layers of the ionosphere that supports a very limited data rate. Under very favourable conditions, a maximum of 9.6 kbit/s user data rate can be achieved in a 3 kHz channel. However, the data rate is normally much lower due to absorption of the signal, manmade noise and interference. Also, rapid time fading and excessive multipath impose a reduced data rate. HF radio systems normally operate in half duplex mode. The advantage of HF communications is extraordinary radio coverage well beyond line-of-sight.

NATO has developed a family of standards at the physical and data link layer within the "HF House" concept. The HF House covers what is called 2G HF technology and 3G HF technology, both of which contain descriptions on *automated* procedures at the link level, appropriate waveforms to be used at the physical level and how the HF subnetwork can interface a data network. Our tests described in this paper have included both 2G and 3G HF technology and also a new data link protocol (HDL+) that will be standardized in the near future. The most important characteristics of the respective HF technologies are described in the following sections.

3.1.1 2G HF

A common operational configuration of a 2G HF system is based on the following set of HF standards: Mil-Std 188 141A [4], STANAG 5066[5], and STANAG 4539 [6]. Mil-Std 188 141A provides automatic link establishment (ALE) in a net of HF radios scanning asynchronously. The link set up may take some time depending on the number of frequencies in the scan set. The waveform used for linking is not particularly robust at low signal-to-noise ratios. When a link is established, the data link protocol defined in S5066 provides efficient and reliable data delivery on a point-to-point link using Automatic Repeat Request (ARQ) and appropriate waveforms defined in S4539. The ARQ scheme is used for adapting the data rate to the channel conditions. The gross data rates provided by the waveforms in S4539 range from 75 bit/s to 9.6 kbit/s. The data link protocol can also be run in broadcast mode where no feedback is provided from the receivers. This does not give a reliable delivery service and eliminates the mechanisms for adapting the data rate.

S5066 defines a subnetwork service interface that consists of a number of service access points (SAP's), including a SAP for IP. IP datagrams must be included in service primitives before delivery over the SAP to the data link protocol. The conversion between IP datagrams and S5066 service primitives is handled by a separate software package, in our case the IP Client software delivered from NC3A [7]. Other SAP's defined in S5066 provide an efficient interface to other applications, for instance HF mail applications such as HMTP and CFTP, without any intervening transport and networking protocols such as UDP/TCP/IP.

For the standards defined above we used the Harris implementation in their RF-5800H radio product and the Harris WMT S5066 software package.

3.1.2 3G HF

For 3G HF, STANAG 4538 [8] includes all the functionalities such as link setup, data link protocol and waveforms. The link setup defined in S4538 is based on all radios scanning a set of frequencies synchronously. The fast link setup (FSLU) used in our tests gives very rapid linking. The waveforms used for link setup are also very robust, enabling linking at negative signal-to-noise ratios. The data link protocol xDL is defined for a point-to-point link and gives an adaptive and reliable data delivery using ARQ and code combining. It is further divided into two classes of protocols called HDL (High throughput Data Link) and LDL (Low latency Data Link). HDL is optimised for delivering large datagrams in medium to good channel conditions and LDL is optimised for delivering small datagrams in all channel conditions and also longer datagrams in poor channel conditions. HDL and LDL use different waveforms with different robustness. The maximum gross data rate for xDL is limited to 4.8 kbit/s, which limits the throughput performance compared to 2G HF. All of the described functionalities of S4538 are implement in the RF-5800H from Harris used in our tests.

S4538 does not currently define a multicast/broadcast mode for packet data. However, the Harris RF-5800H radio provides a proprietary broadcast packet service where the data rate is fixed.

No subnetwork service interface is currently described in S4538. In the Harris implementation, there is a direct IP interface at the radio, supporting both Ethernet and PPP, and making the radio act as an IP router. Applications using IP services may therefore connect directly to the radio.

3.1.3 The new data link protocol HDL+

A new data link protocol has been proposed by Harris to become a part of S4538 in the future. HDL+ is a point-to-point protocol and will to a large extent replace HDL, providing higher throughput and lower latency on good HF channels. The protocol has been designed to remove the data rate limitation of S4538 and to support an efficient exchange of IP based data traffic. The same efficient link setup is used for HDL+ as for 3G HF. The data link protocol combines the high data rate waveforms of S4539 with some code combining technique, and gives an adaptive data link protocol capable of error free delivery up to 10 kbit/s in a 3 kHz channel [9]. For poor channels the HDL+ has no potential gain compared to the LDL protocol in S4538, and the Harris implementation resorts to LDL. The same IP interface as for 3G applies to the HDL+ protocol.

3.2 IP over HF

The communications scenario we discuss in most of this paper is described in Figure 2. An HF link is used to connect the IP networks A and B. Two data terminals are hosting a S4406 Message Transfer Agent for provision of a seamless MMHS service to the mobile platform. The nodes HF A and HF B each comprise the HF radio/modem functionality, the HF link protocols, an optional link crypto functionality and finally an IP routing functionality.

Compared to most other links used in an IP network, the throughput of a typical HF link will be very low and variable, and the latency will be very high. In order to take advantage of the IP service offered by the HF radio link, the protocols above the network layer must be able to tolerate the high latency imposed by the HF link protocols. TCP is not particularly suitable for use over HF because of the variable capacity of HF requiring conservative timer settings and because the cost of reversing the channel at HF is rather high. In most cases the HF link will inevitably represent a bottleneck in the IP network with a great impact on the quality of service being offered to the user.

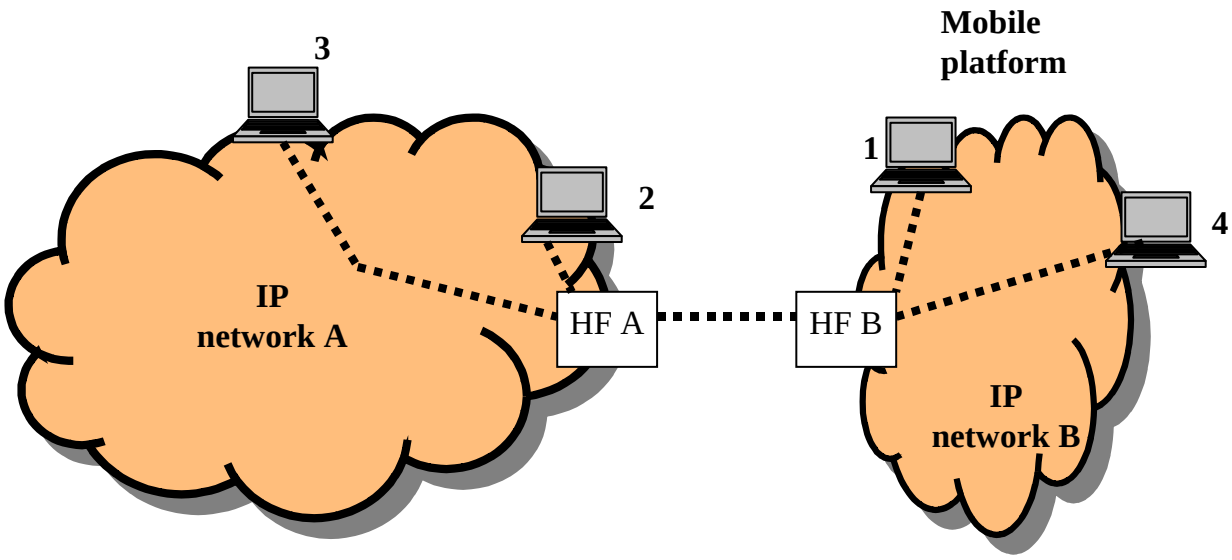


Figure 2: Model of IP networks connected by HF

4.0 PERFORMANCE OF THE NATO MESSAGING APPLICATION OVER HF LINKS

The aim of this study has been to explore the efficiency of the message transfer of the MMHS by using a transparent IP service over the different HF technologies and to understand the interactions between the protocols. Focus has been on efficiency over a point-to-point link, and measurements have been conducted in both the laboratory and over-the-air. Earlier published results can be found in [10], [11] and [12]. We have also addressed the Multicast properties of S4406 Annex E utilizing the Harris proprietary Broadcast protocol of RF-5800H. Laboratory measurements illustrate a few points about the efficiency of Multicasting over HF.

4.1 Recapitulation of earlier published results

Our first investigations were conducted in the lab under controlled channel conditions. The test setup was similar to the setup shown in Figure 3, except that the radios were connected with attenuators, and there was no need for a modem to control one of the radios. White Gaussian noise was inserted at a controlled level at the inputs of each radio, but no fading model was used. A frequency set consisting of ten frequencies has been used throughout the tests.

Figure 3 shows the test setup for the over-the-air tests that were conducted between Lillehammer and FFI at Kjeller, a 140 km path in southern Norway. A modem over the telephone network enabled us to control and monitor the message reception at the remote site, and transfer times were recorded. The power transmitted was 125 W and the antennas were broadband dipoles.

Thales XOmail (S4406) was located at the PC's together with the WMT S5066 software. For the 2G tests, a second PC hosted the IP Client software on each side.

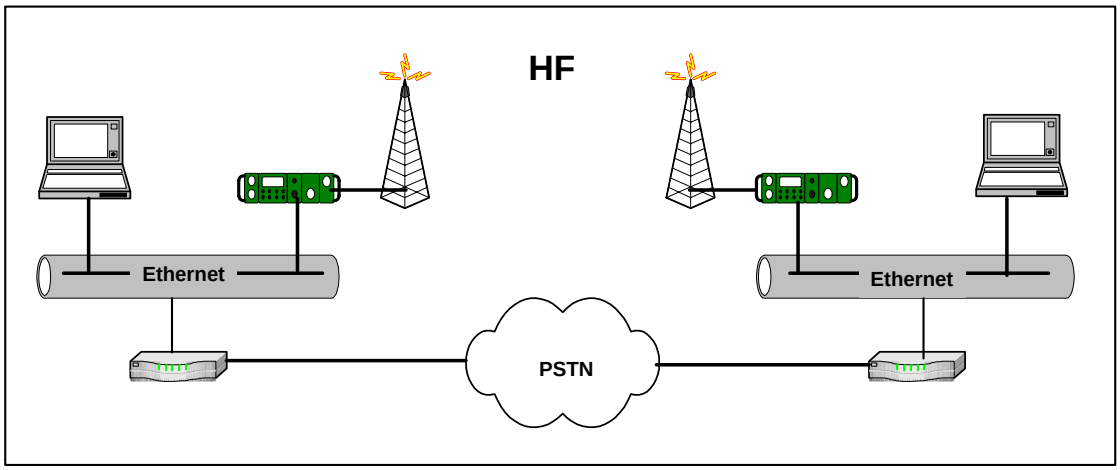


Figure 3: Over-the-air test setup

Compressed messages were transferred between the messaging application at each site, and the transfer times were recorded. The *application level throughput* was calculated as the compressed message size divided by the delivery time. Since the message is delivered before all the protocol layers have been released, the throughput calculations are slightly optimistic, in particular for short messages. Each measurement was repeated around 10 times and averaged. ALE/FLSU are included in the measured transfer times and in the throughput calculations.

4.1.1 Throughput

Comparing the througput performance on a "perfect" channel of the Annex C (strategic) and Annex E (tactical) protocol profile over S4538 (3G HF) shows that Annex E improves the throughput by a factor of six for a 400 byte file and by a factor of 2 for a 75 kbyte file. The improvement factor increases as the HF channel deteriorates, so that on a typical HF channel, the improvement factor will be higher than the figures mentioned here. In the following, only the Annex E protocol profile has been tested further since it outperforms the Annex C profile over an HF link.

We observed that transfer times (and therefore throughput) were affected not only by the protocols in use and the channel conditions. Also implementation choices made by the equipment vendors and configuration parameters selected by the user, contribute to the transfer times. For instance, the HF standards define a number of different waveforms, but the choice when to use the different waveforms is up to the vendor. Also frequency selection algorithms, buffer size and buffer handling are implementation dependant. Moreover, the transfer times depend on configurable parameters of the application such as PDU size and packet rate. Consequently, the throughput measured is only indicative of what can be obtained, and does not serve as a definite upper limit.

Our next observation focuses on the different HF link protocols (2G, 3G and HDL+) as the carriers of S4406 Annex E message traffic. We measured application throughput for various file sizes ranging from 400 bytes to 75 kbyte over an error-free channel. The results are shown in the leftmost panel of Figure 4. For message sizes below 10-20 kbyte, the HDL+ protocol gives twice as much throughput as the 3G and the 2G protocol. The 2G protocol suffers from in-efficient linking using Mil-Std 188 141A, and the 3G protocol suffers from low data rate waveforms. For larger message sizes (>20 kbyte) the effect of in-efficient linking for 2G is reduced and 2G performs at the same level as HDL+, but 3G still suffers from low rate waveforms. We will come back to the dip in throughput around message sizes of 20 kbyte for HDL+/3G in the next section. The rightmost panel of Figure 4 shows the application throughput versus signal-to-noise ratio on the channel for a fixed message size; 9.3 kbyte. At positive SNR's the HDL+ protocol provides the best performance whereas HDL+ and 3G provides similar results at negative SNR's. The 2G link establishment is less robust than 3G/HDL+, and linking is not achieved at negative SNR's.

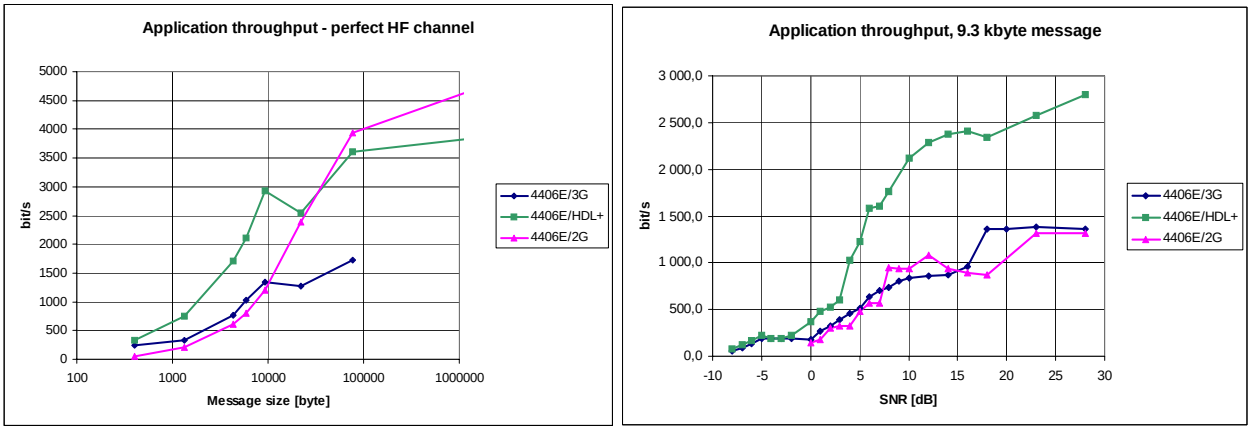


Figure 4: Comparison of throughput vs message size (left) and comparison of throughput vs SNR for a 9.3 kbyte message (right)

To compare the performance of the different HF protocols as bearers for S4406 traffic *over-the-air*, the protocols were tested in sequence but within a maximum time period of three hours. At the start of measurements for each protocol, channel quality scores in the radios were updated by channel soundings allowing an optimum frequency selection. Measurements were conducted in March/April 2004 under benign conditions, the local geomagnetic K index was never above 3 for the data shown in this paper.

However, the diurnal variability of the HF channel was quite noticeable. Figure 5 shows averaged application throughput vs time of day for a message size of 9.3 kbyte (left) and 22 kbyte (right).

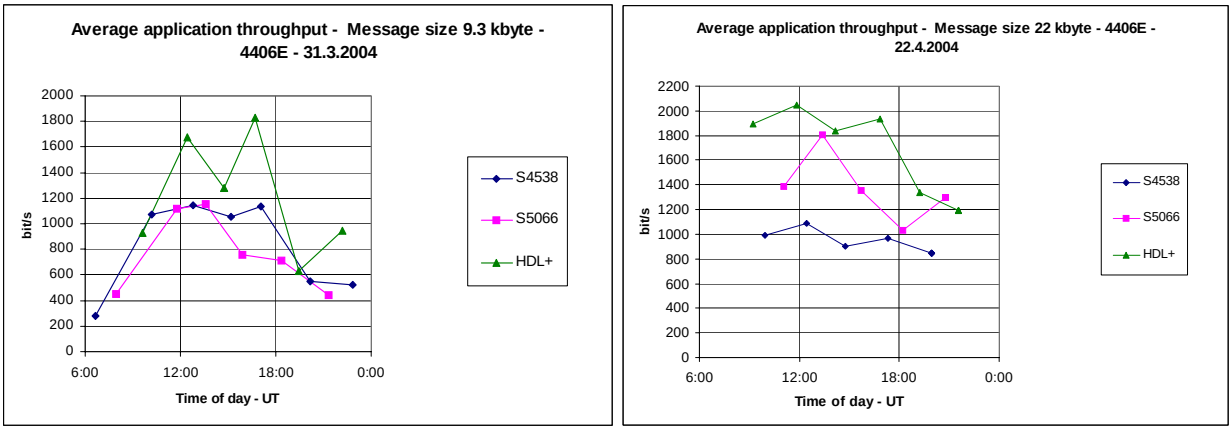


Figure 5: Comparison of throughput over-the-air vs time of day for a 9.3 kbyte message (left) and a 22 kbyte message (right)

The following conclusions can be drawn from the over-the-air tests of S4406 over the various HF protocols:

- Under good day time conditions (SNR > 20 dB) the measured average throughput for HDL+ remained well below the simulated throughput of 4500 bits/s for a 5 kbyte message on an ITU poor channel referred in [9]. Our results include the effect of non-optimum offered load from an application and realistic channel conditions which may be worse than the ITU poor channel.
- The variation of the message transfer times (and therefore throughput) when transmitting 10 consecutive messages for each HF protocol, is significant.
- The automatic channel selection algorithm of the radio is very important for achieving high throughput.
- The difference between the measured performance of the HDL+ protocol and 2G is primarily caused by the less efficient linking protocol of the 2G, and the effect of this is lower for larger message sizes.

4.1.2 Congestion control aspects

Referring to Figure 2, IP packets may arrive at the HF transmit node at a higher rate than the node is able to support, and hence, packets will accumulate in buffers at the HF node. With respect to the throughput of the HF link this is desirable, because the HF protocol efficiency improves with full radio buffers. However, since neither P-Mul nor UDP has mechanisms for network congestion control, buffers in the HF transmit node will tend to overflow, and packets will be discarded for long messages. The discarded packets will be retransmitted by P-Mul, but this effect may severely deteriorate the overall performance of the Annex E protocol stack.

The present XOmail implementation of ACP 142 P-Mul protocol and the IP service of the RF-5800H come around this problem by introducing a “local” congestion control mechanism, which makes use of the IETF standard “IP Control Message Protocol” (ICMP) (13). When the buffer of the HF transmit node overflows, an ICMP Source Quench message is generated and sent to the originating end terminal. This message will instantaneously stop the packet flow from P-Mul, thereby minimizing the influence of the buffer overflow. A timer will start the packet transmission again.

The buffer size of the RF-5800H in our 3G and HDL+ setups is about 10 kbyte. For message sizes exceeding the buffer size, a packet is discarded before the Source Quench is effectuated with a following reduction in throughput as seen in Figure 4 (left). The buffer size of the IP Client of the 2G HF subnetwork (software on a PC) is much higher, and no packets are discarded in the 2G measurements.

Although not perfect, by using the Source Quench mechanism for congestion control a reasonably high throughput capability will be achieved also when transferring long messages. However, there are unresolved issues regarding the use of the Source Quench mechanism. A new version of ACP 142 is under development by NATO and the CCEB, which will include functionality for end-to-end congestion control (see section 6.1).

4.2 Multicast

The broadcasting nature of radio nets can be utilized to offer an IP multicast service. This implies that IP data packets are broadcasted over the radio net and delivered to those addresses defined by the IP multicast address. In its simplest and most common form a multicast link service is based on broadcasting without link acknowledgements/retransmissions, and hence provides a less reliable service than unicasting. Multicasting may provide a potentially bandwidth efficient transfer capability, especially when there are many recipients of a message in the same radio network.

2G HF (S5066) offers a broadcast packet service. The 3G HF (S4538) in its present version does not. However, the implementation of S4538 from Harris that we are using in our tests, extends the present S4538 to provide a simple IP broadcasting service, on which a limited IP multicast service can be based. One of the key features of the STANAG 4406 Annex E is the multicast ability of the P-Mul protocol. We have done some introductionary testing to investigate how well this protocol will work on an HF network with S4538 extended with the IP broadcast protocol.

A multicast message transfer from A to three recipient nodes B – D has the following phases:

1. Transfer of the P-Mul Control PDU and the P-Mul traffic PDUs from A. Radio A sets up a channel on a suitable broadcast frequency and sends these PDUs by IP broadcasting at a fixed data rate.
2. Transfer of the P-Mul ACK/NACK control packets from each of the nodes B – D by using the S4538 unicast service.
3. Unless all the nodes have given a positive acknowledgement, P-Mul at node A will retransmit missing PDUs, and the nodes B – D will update their acknowledgement status. This repeats until all the nodes have received all PDUs from A.
4. When the P-Mul entity of node A has received acknowledgements from all the addressees, it will send an end-of-message (EOM) by IP broadcast, terminating the message transfer.

Thus, all P-Mul packets transmitted from node A use the IP multicast service, whilst the individual P-Mul ACK/NACK packets in the reverse direction use the unicast service. While the latter is a robust service with adaptable data rates and link acknowledgements, the former is a fixed data rate service without link acknowledgements. Hence the probability of delivery of a multicast message is strongly dependent on the fixed data rate selected for the channel. Unless a relatively low data rate is chosen for the broadcast channel, the IP multicast service will not be very effective in delivering messages to addressees that are operating on HF channels with low SNRs. For example, as a guideline, by using a data rate of 600 bit/s, HF channels with an SNR of a few dB's are required for acceptable delivery of multicast traffic. Increasing the rate to 4 800 bit/s increases the SNR requirements by about 10 dB.

Figure 6 shows a picture illustrating the difference in channel activity between the IP unicast service and the IP multicast service in the case of S4406 Annex E sending the same 2.5 kbyte message to 3 message

recipients over an HF channel with an SNR of 6 dB. The IP broadcast data rate is 600 bit/s. The unicast service (left panel) handles the message transfer by sending the messages sequentially to one recipient at a time. The multicast message (right panel) is sent once and is delivered to all the recipients at the same time. The recipient nodes release their P-Mul acknowledgements approximately simultaneously, resulting in all three trying to set up a link to the originator at the same time and creating some havoc on the channel in this process. The S4538 protocol is able to resolve this channel allocation conflict, but it is noted that a very long time is spent for the transfer of the three ACK messages. In the end the originating node broadcasts an End of Message PDU terminating the P-Mul session.

The figure shows that in this given situation, less radio resources are needed when the IP multicast service is used to deliver the message. The message delivery time of the multicast message is about half of the average delivery time experienced when using three unicast messages. However, the P-Mul acknowledgement transfers taking place right after the multicast message delivery, are handled rather inefficiently by the protocols. The accumulated seizure time of the HF channel is still about 40% lower than for the unicast service in the above scenario, thus easing the load on the HF resources. This advantage will increase for an increasing number of message recipients. However, if the channel quality improves, the message transfer times for the unicast service will decrease because of the adaptive data rates, whereas the multicast service is stuck with the fixed data rate. This may change the picture of multicast using HF resources more effectively than unicast.

There are room for performance improvements for the handling of multicast traffic, as regards the implementation of the HF protocols as well as XOmail protocols. We believe that the use of S4406 Annex E combined with an efficient multicast link protocol has the potential of providing attractive solutions for several one-to-many HF communications scenarios.

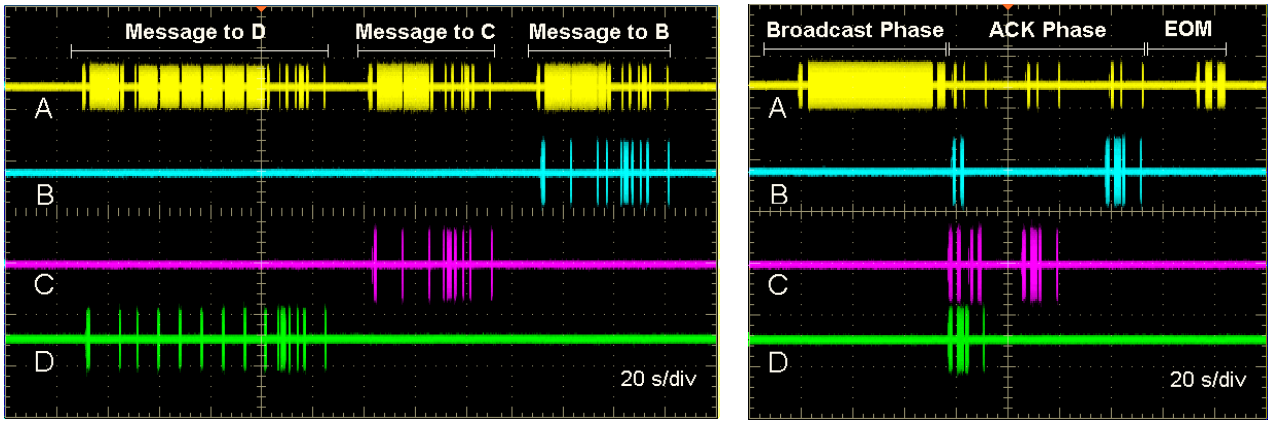


Figure 6. Oscilloscope traces showing the transmissions from the four HF radios when a message is sent to three destination addresses. The left/right panels show the activity when the message is sent as three unicast messages or as multicast, respectively. The upper trace represents the sending node.

5.0 A COMPARISON WITH A DEDICATED HF MESSAGING APPLICATION FOR UNICAST MESSAGE TRANSFER

The results presented so far are all based on the transparent transfer of IP packets carrying S4406 Annex E information wrapped in UDP PDUs over the HF links. There are, however, other options for transferring information over an HF link. As mentioned, S5066 defines a set of Service Access Points (SAP), some of which may be used to map the application information directly to the HF link level. Two of these are optional SAP's defined for use by the HF mail Transfer Protocol (HMTP) and the Compressed File

Transport Protocol (CFTP), respectively. Both of these protocols are made for efficient packaging of messages for HF transfer. However, this solution of a direct mapping of the application information to the HF link layer does not provide any networking functionality. Consequently, such a solution is only viable over a one-hop HF link.

It would be reasonable that mapping application information directly to the HF link layer requires less HF capacity than if UDP/IP is involved. Hence it is to be expected that S4406 Annex E using a transparent IP service would be less efficient than using CFTP/HMTP mapped directly to HF. We used the Wireless Message Terminal RF-6710W (WMT) from Harris to send a message with a compressed attachment by CFTP over S4538, so that a comparison with XOmail using transparent IP over HF to send the identical message could be made. However, such a comparison is indeed a bit like comparing “apples and pears”, since it does not account for the inherent advantages of the S4406 Annex E with respect to its offering of military services such as security and priority, or to the seamless interoperability it offers with military strategic messaging systems and with military procedures.

The following parameters were compared:

- the message delivery time.
- the total time duration that the HF channel is linked for the complete message transfer. This expresses the required use of HF resources for the message transfer.
- the number of bytes additional to the size of the compressed file that the S4538 has to transfer. This is a measure of how efficient the message is packaged at protocol levels above the datalink layer.

The measurements were made with a channel SNR of 20 dB. Figure 7 shows the measured performance parameters of S4406 Annex E (XOmail) using the transparent IP service over S4538 relative to the measured performance parameters of CFTP (WMT) mapped directly to the S4538 link protocol. It should be noted that the measurements do not only reflect the contributions from the standardized protocols, but are also affected by implementation choices and to some degree by processing times. One such important implementation parameter is the procedures and timer values used in conjunction with IP transfers over S4538. These are not part of S4538, and we believe there is some room for improvements in the efficiency of IP transfers of the measured equipment.

The green curve in the figure shows that the increase in the HF data link payload of the S4406 Annex E is very modest and only occurs for short messages. We assume that this increase may be at least partly explained by the added information that needs to be transferred due to the military services offered. The S4406 Annex E over IP also gives a slight increase of the message transfer time (blue curve). This percentage increase in transfer time grows with increased message size. This is primarily caused by the fact that the S4538 implementation organizes the IP traffic less efficiently than for bulk message transfer. The IP packets are organized in assemblies. Between each assembly there is a time gap in order to allow for channel reversal, and this time gap results in reduced protocol efficiency.

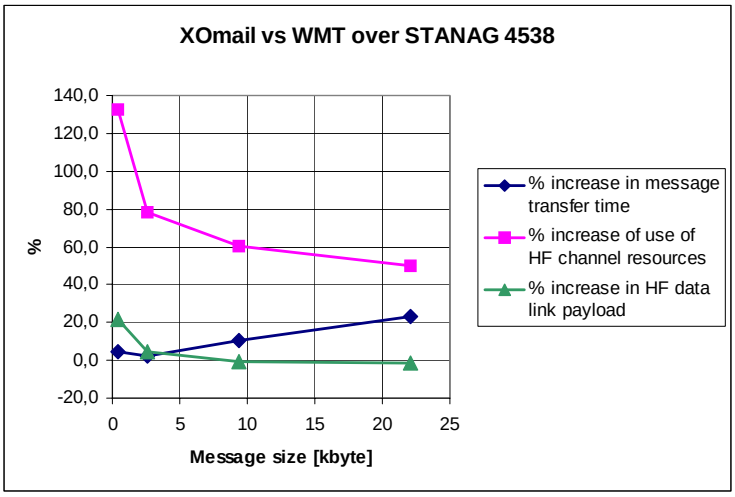


Figure 7. The performance of XOmail using a transparent IP service relative to using the WMT (CFTP) mapped directly to S4538.

The pink curve showing the most dramatic difference is related to the use of the HF resources, i.e the total time that the HF channel is occupied during one complete message transfer. There is a simple reason for this, which is the end-to-end acknowledgment mechanisms which are part of the Annex E protocol. The transmission of a P-Mul ACK in the reverse direction followed by a P-Mul EOM secures the S4406 Annex E message delivery reliability in an optimum manner. However, two channel reversals are necessary to accomplish this, and it is basically these channel reversals/HF link management messages that causes the use of the HF channel resources to increase sharper than the message transfer time. The WMT does not make use of a true end-to-end acknowledgement concept. It conveyed only the one-way message content on the HF channel.

The measured increase in message transfer time and the increased use of HF resources for the measured S4406 Annex E system are to a large extent attributable to its use of a transparent IP service and to the way that this service is handled by the implementation of the HF link protocol. Using the transparent IP service is a general solution, enabling HF to become an integrated part of the tactical internet. However, a solution with application data mapped directly down to the HF link layer will provide some efficiency gains. Such a gain may be provided also for S4406 Annex E systems, since there exists an option for a S4406 Annex E HF subnet interface SAP similar to those defined for CFTP/HMTP. As mentioned, the above comparison only considers the efficiency aspect of the message transfer. It must be kept in mind that important differences in functionality and service level between the systems are not reflected.

6.0 PROPOSALS FOR IMPROVEMENT OF THE P-MUL PROTOCOL (ACP 142)

We have experienced limitations of the current P-Mul protocol and implementation in our testing. A new version of ACP 142 is under development by NATO and the CCEB. Proposals have been made to include new functionality such as end-to-end congestion control, Forward Error Correction (FEC), handling of acknowledgement implosion and more dynamic mechanisms for adaptation of timers to the change in the communications conditions of disadvantaged grids. Since the proposals are still under discussion at the time of writing, some of the proposed functionality will be presented here without going into details.

6.1 Congestion control

In the current version 1.0 of the ACP 142 protocol, there are no congestion control mechanisms specified. The requirement for a congestion control mechanism and how it is solved using the IETF ICMP Source Quench protocol in the XOmail application and the RF-5800H radio is described in section 4.1.2. Since the congestion control problem is at the transmitting side between the application and the radio and not between the sending and receiving application, this form of congestion control is reasonable to use because it addresses the problems locally. However, because the ICMP Source Quench will not be maintained for IPv6, and the potential use of IP crypto will prevent the ICMP Source Quench packet from being transmitted from the radio to the application, another mechanism will have to be chosen. An end-to-end congestion control mechanism is being discussed for the next version of ACP 142. This solution will most likely be based on calculation of the measured delays of the P-Mul PDU's, which then will be used to regulate the flow of PDUs being sent from the P-Mul protocol. Timestamps may be added to some of the P-Mul PDUs in order to log the transfer time, which then is reported back to the sender. Such an end-to-end congestion control mechanism will not be as adaptable to the change in the communication conditions as the local ICMP Source Quench mechanism, because of the delay in getting the response. There are however, not many other alternatives if the use of IP crypto is not to be prevented.

6.2 FEC

An optional FEC mechanism in P-Mul is proposed. The main intention of the FEC is to improve the protocol performance on channels that are susceptible to PDU loss. This is the case when using radio channels with no acknowledgement mechanisms, for example when sending to EMCON recipients or when using a simple multicast protocol on a broadcast channel.

By introducing the FEC mechanism the complete message may be reconstructed by the recipient, even if a certain number of P-Mul PDUs are lost. This will increase the probability of message delivery to EMCON recipients. When using the multicast service with the FEC option, fewer (or no) negative acknowledgements will be required. In some cases, in particular when using HF protocols, the cost of returning an acknowledgment PDU may be high, and a reduction of the P-Mul traffic gives a noticeable performance improvement. On channels susceptible to PDU losses, a shorter delivery time is achievable by using the FEC option.

Reed-Solomon codes have been proposed as a suitable FEC mechanism at the P-Mul layer, due to its flexibility and its powerful error correcting capabilities.

6.3 More dynamic parameters for adaptation to the communication conditions

The current version 1.0 of the ACP 142 protocol uses static parameters that may cause problems when the protocol is used over radio systems with varying data rates end error conditions.

One of these static parameters is the re-transmission timer, which has to be set high if the condition of the channel is varying, in order to avoid premature time outs and retransmissions in the worst-case situations. A proposal has been made to make this timer more adaptable by taking into account the measured round trip delay and the size of the message to be transferred.

Another dynamic parameter proposed is the "Receiver Last PDU Timer". In the current version of the ACP 142 protocol, an acknowledgement is triggered by the reception of the last Data_PDU expected by the receiver. This means that if the last Data_PDU is lost, the receiver will not generate an acknowledgement. This will cause the transmitter to time-out and start re-transmitting the data. The new timer will trigger the generation of an acknowledgement if the last Data_PDU is lost, and will be calculated dynamically based on the arrival time of the previous Data_PDUs.

6.4 Handling Ack Implosion

If a message is multicasted to many recipients, there is a problem that the recipients may start sending acknowlegements at the same time. In radio networks, this may result in collisions because they all try to access the channel. In order to avoid this situation, there is a proposal for the next version of ACP 142 that all recipients are waiting a randomized period of time before sending the acknowledgement.

7.0 CONCLUSIONS

In the migration process towards NATO Network Enabled Capabilities, the MMHS based on STANAG 4406 may offer a seamless connectivity between NATO nations, between strategic and tactical units and between services. The MMHS is a tool for military command and control which, with the inclusion of Annex E, is extended to tactical users. The MMHS application may be used over different networking technologies and bearer services. By using the S4406 Annex E protocol profile we have shown that a reliable and reasonable message transfer is possible over an IP network which comprise an HF link. This opens for an architecture where the HF links may be directly utilized also for IP traffic from various other applications. This is not possible with mail applications dedicated for a specific radio link such as HF. However, the latter solution is able to utilize the HF channel resources more efficiently.

MMHS Annex E over HF systems is a viable solution, providing application throughputs up to a few kilobits per second. However, an HF link will represent a potential “bottleneck” in an IP network and it requires special attention for optimum performance. We experienced congestion control problems when using UDP/IP over a narrowband tactical link such as HF. Acceptable performance was achieved by using a congestion control mechanism based on ICMP Source Quench, but in the long term a new congestion control mechanism is called for.

The multicast functionality of S4406E promises to be an efficient way of delivering one-to-many traffic when used in conjunction with a suitable HF link service. In a simple one-to-many scenario tested, a significant reduction in the mean message delivery time was achieved and less radio resources were needed by transferring the message by an IP multicast service rather than by consecutive IP unicast transfers. The multicast performance can be enhanced further by modifications of the P-Mul protocol as well as in the RF-5800 IP broadcast protocol.

It is important to test complete systems together, ranging from application to the physical link. There are optimisation issues at different levels of the protocol stack, and we have seen that implementation choices and parameter setting have great impact on the overall performance of the system.

8.0 ACKNOWLEDGEMENTS

Thanks to Harris Corporation and Thales Norway, for technical support of this work.

9.0 REFERENCES

[1] NATO Standardization Agreement (STANAG) 4406, Military Message Handling System (MMHS), Ed. 1, 1999

[2] Allied Communication Publication (ACP) 123, Common Messaging Strategy and Procedures, Combined Communications Electronic Board (CCEB)

[3] Allied Communication Publication (ACP) 142 v 1.0, P-Mul: An application for Multicast Messaging under EMCON Restriction, 2000

[4] US Mil-Std 188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment, Appendix A

[5] NATO Standardization Agreement (STANAG) 5066, Profile for High Frequency (HF) Radio Data Communications, Version 1.2

[6] NATO Standardization Agreement (STANAG) 4539, Edition 1, Technical Standards for Non-hopping HF Communications Waveforms

[7] Smaal J W, Application Note: STANAG 5066 IP Subnet Client, SISmcast, NC3A, http://elayne.nc3a.nato.int

[8] NATO Standardization Agreement (STANAG) 4538, Edition 1, Technical Standards for an automatic Radio Control System (ARCS) for HF Communications Links

[9] Chamberlain M W, Furman W N, HF Data Link Protocol Enhancement based on STANAG 4538 and STANAG 4539, Providing Greater than 10 kbps Throughput over 3 kHz Channels, *IEE Conference Publication No 493*, pp 64-68, Bath, UK, 2003

[10] Jodalen V, Solberg B, Eggen A, Grønnerud O, IP over HF as a Bearer Service for NATO Formal Messages, *IEE Conference Publication No 493*, pp 19-24, Bath, UK, 2003

[11] Jodalen V, Eggen A, Solberg B, Grønnerud O, Military Messaging in IP Networks using HF Links, *IEEE Communications Magazine, Vol 42, No 11*, pp 98-104, Nov 2004

[12] Jodalen V, Solberg B, Grønnerud O, On-air Testing and Comparison of 2G and 3G HF, *Nordic HF Conference Proceedings*, p 3.5.1, Fårø, Sweden, 2004

[13] IETF RFC 792,"Internet Control Message Protocol (ICMP)"

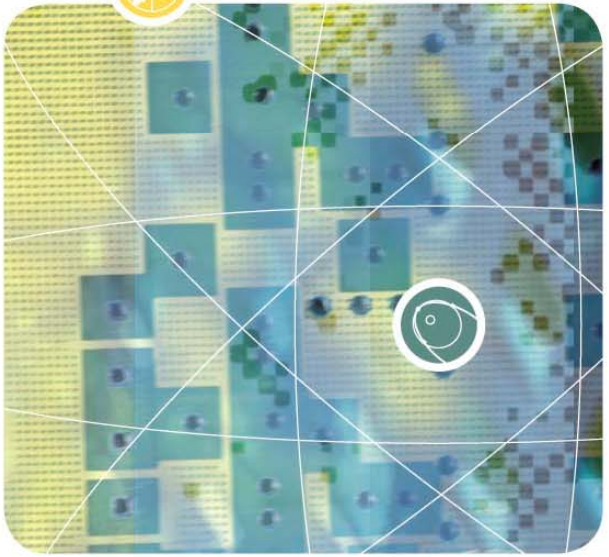
FFI Forsvarets forskningsinstitutt

NATO Military Messaging in the Tactical Domain

- performance issues of an HF channel

RTO/IST Symposium
Rome, Italy
18th - 19th of April 2005

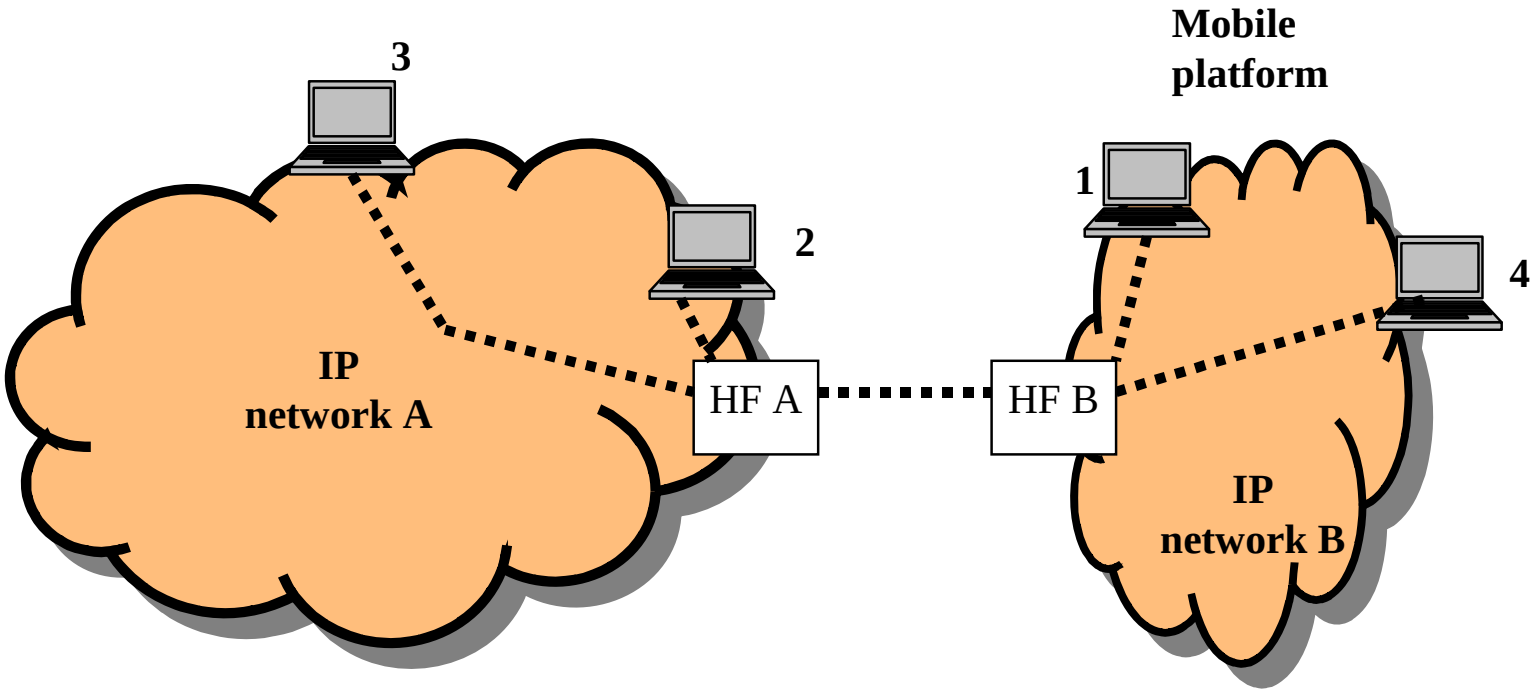
Vivianne Jodalen,
Anders Eggen,
Bjørn Solberg,
Ove Grønnerud, FFI



Contents

- NATO Military Message Handling System (MMHS)
- Automated HF systems
- MMHS using IP over HF on a point-to-point link
  -laboratory measurements
- IP Multicasting over HF
- Comparison between the MMHS and a dedicated HF messaging application
- Conclusions

IP networks connected by HF



The application: NATO Military Messaging

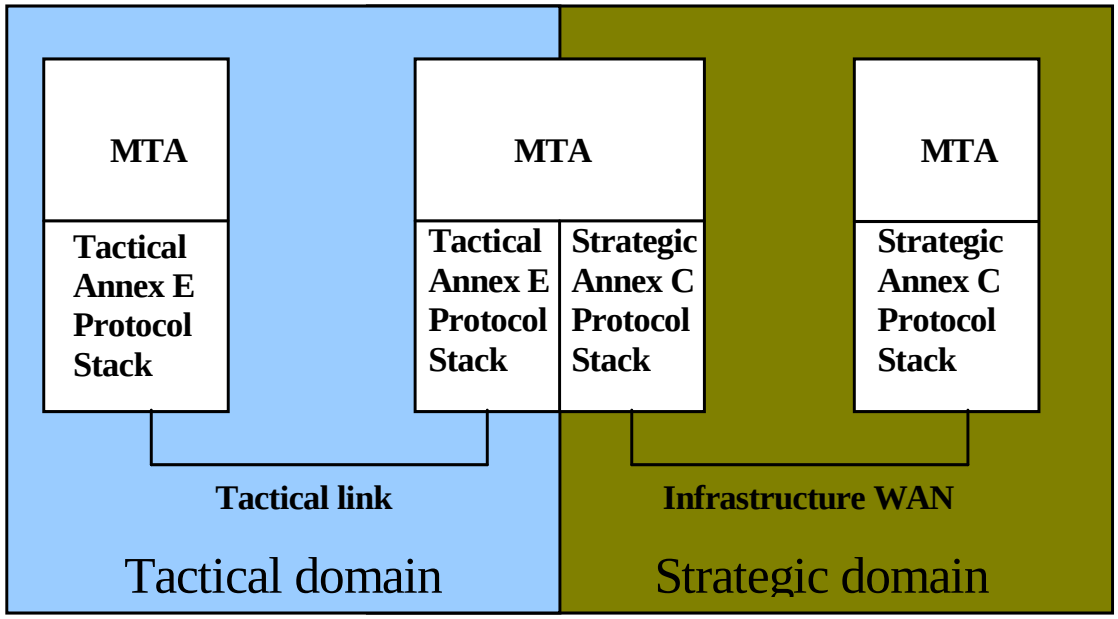
Formal Military Message
is different from an interpersonal message in that it is a message:

- sent on behalf of an organization
- sent in the name of that organization
- that establishes a legal commitment on the sending and receiving organization under military law
- that has been released and handled in accordance with strict policies and procedures of the orginating nation

Military Message Handling System (MMHS)
handles Formal Military Messages

STANAG 4406
is the only agreed NATO standard for formal military messaging

MMHS in the tactical environment



With STANAG 4406 Annex E, a common baseline protocol solution exist that may be used between the strategic and tactical environment and within the tactical environment

Technical characteristics of the STANAG 4406 Annex E application

- requires a connectionless transport service (e.g. UDP/IP)
- selective acknowledgement at application level
- multicast or unicast (ACP-142, P-Mul)
- handles EMCON and non-EMCON recipients
- no flow control mechanisms are defined in the current version of ACP-142

HF Communications

- Extraordinary radio coverage well beyond line-of-sight
- 3 kHz channel allocations giving a maximum gross datarate of 9.6 kbit/s under very favourable conditions
- Variable channel conditions depending on time, location and other users of the spectrum
- Half duplex channels giving large turn-around times

- A family of HF standards at the physical and the data link layer has been agreed upon in NATO (”HF House”)
- Includes automatization of channel selection, link establishment, link maintenance and adaptive data rate

Automated, standardized HF systems

2G HF

- Mil-Std 188-141A
- STANAG 5066 including subnetwork service interface with an IP SAP
- STANAG 4539

Slow and non-robust linking, max gross datarate of 9.6 kbit/s

3G HF

- STANAG 4538

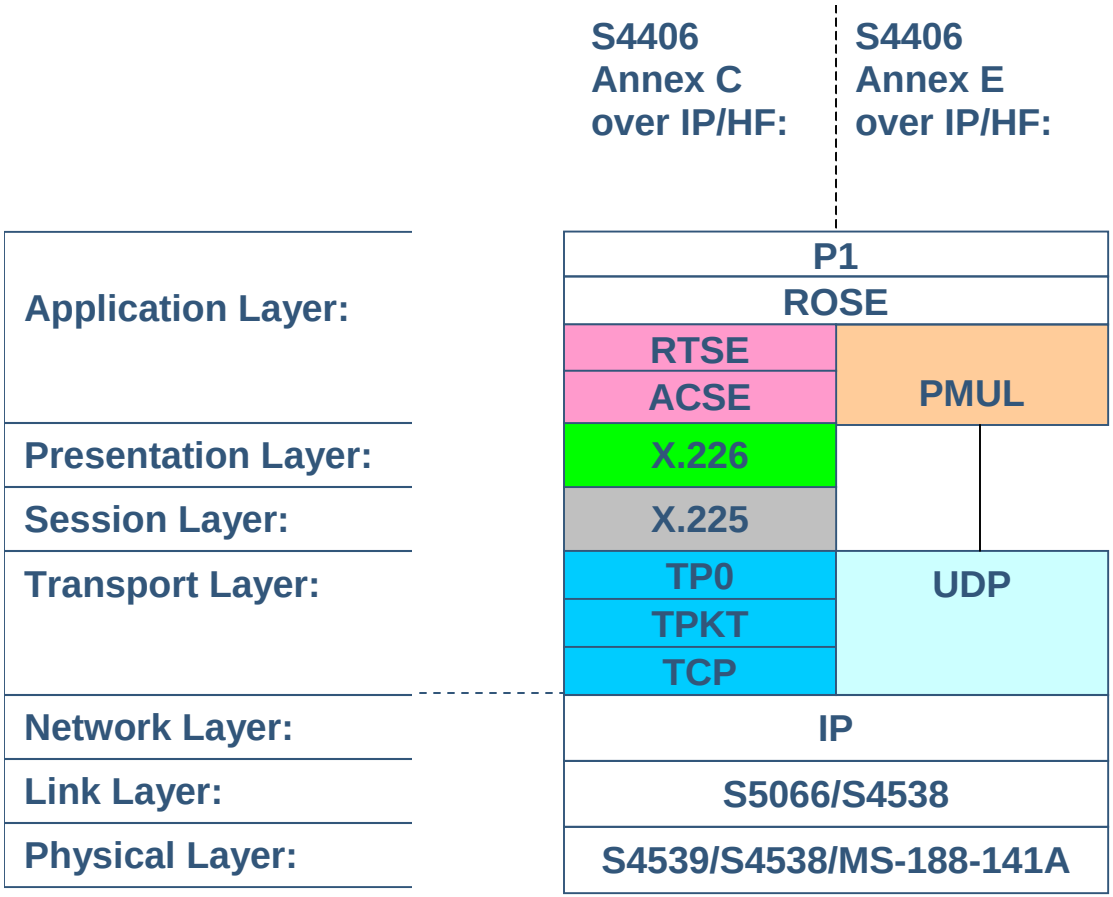
Rapid and robust linking, max gross data rate of 4.8 kbit/s

HDL+

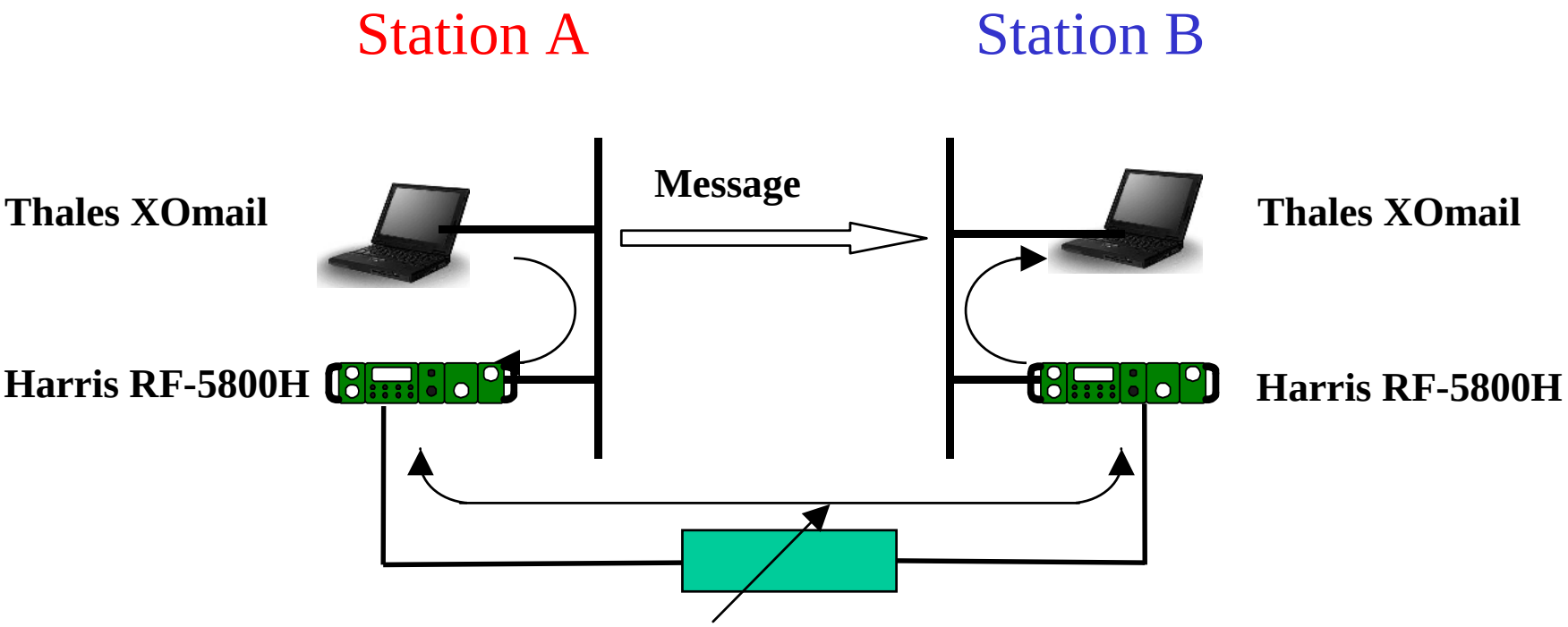
- based on STANAG 4538, proposed for standardization by Harris Corp.

Enhanced efficiency and max gross data rate of 9.6 kbit/s

STANAG 4406 Annex C and E over IP/HF



Test setup for MMHS over S4538 and HDL+



Radio buffer overflow

Ethernett

Radio buffer →

HF

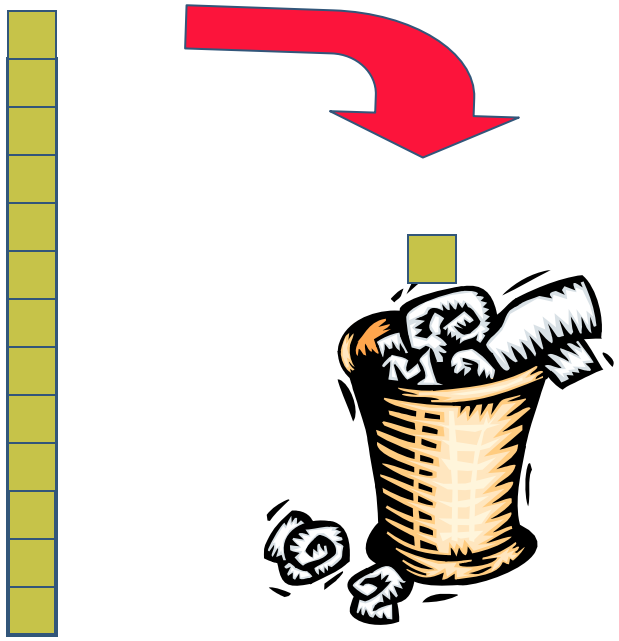
Radio buffer overflow

Radio buffer overflow

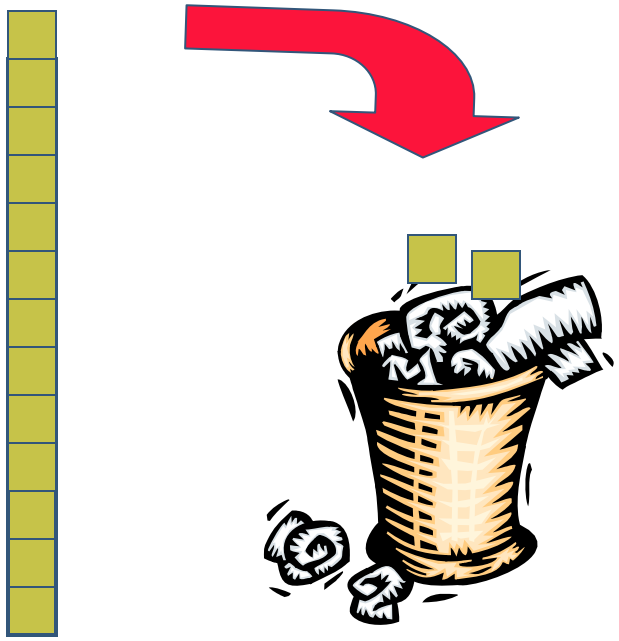
Radio buffer overflow

Radio buffer overflow

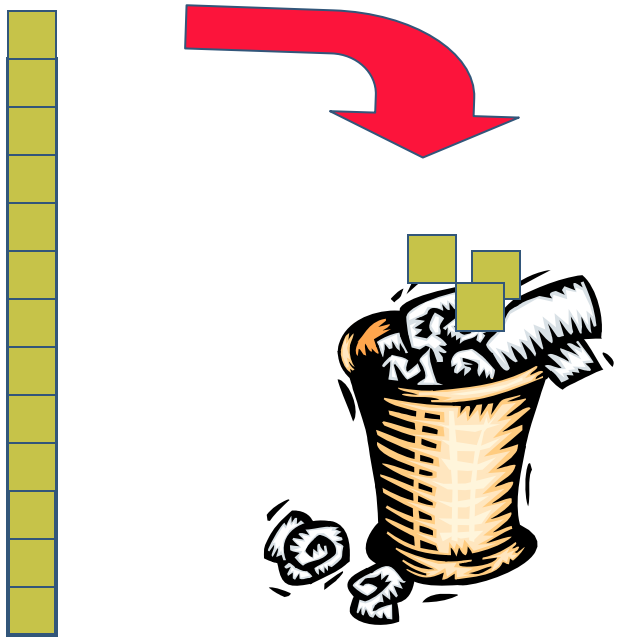
Radio buffer overflow



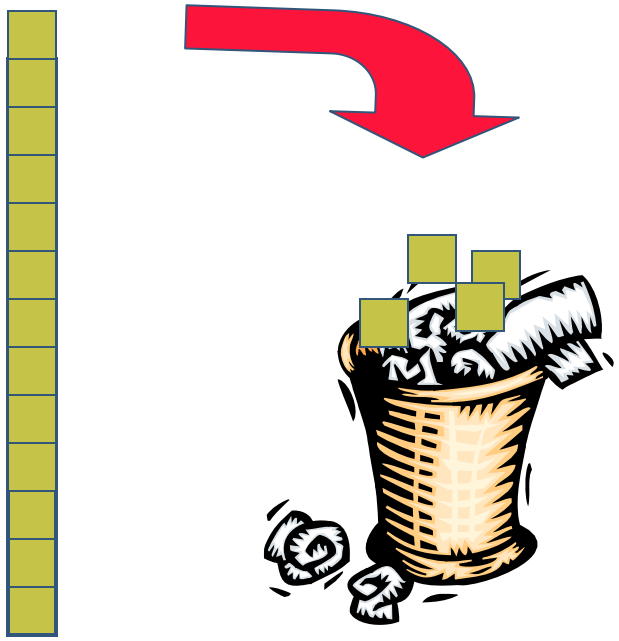
Radio buffer overflow



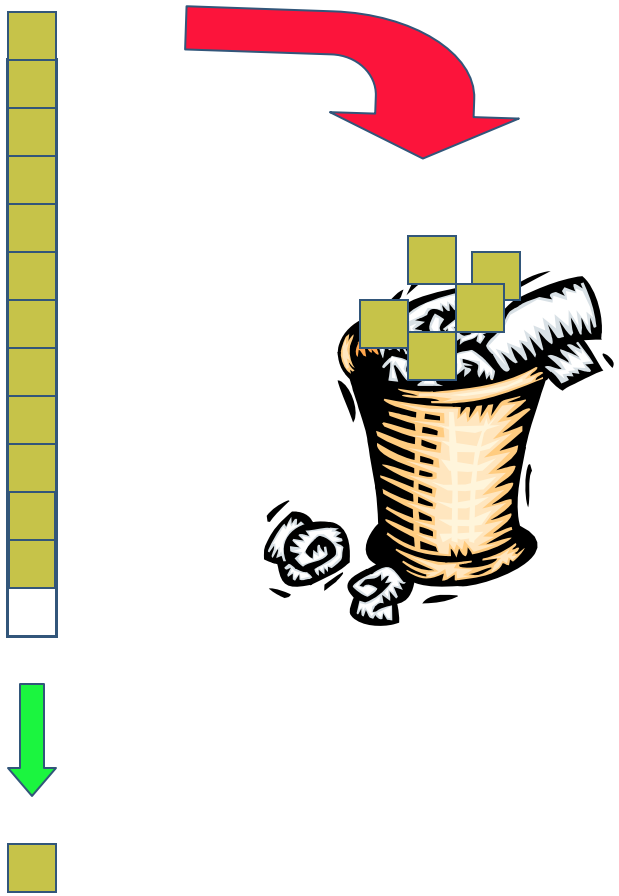
Radio buffer overflow



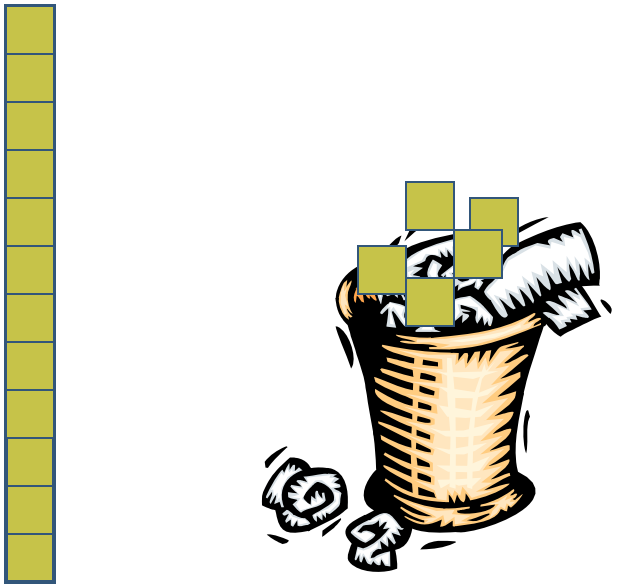
Radio buffer overflow



Radio buffer overflow



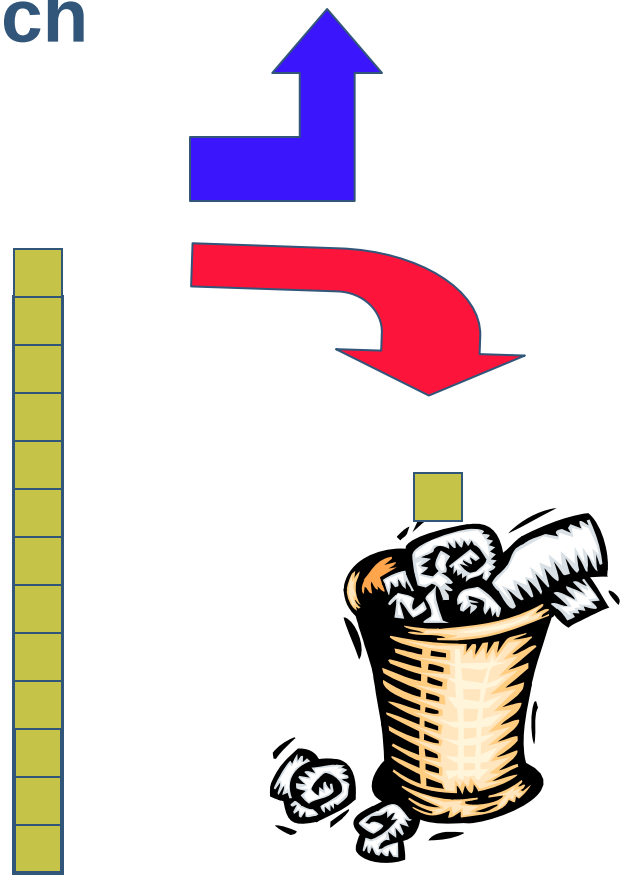
Radio buffer overflow



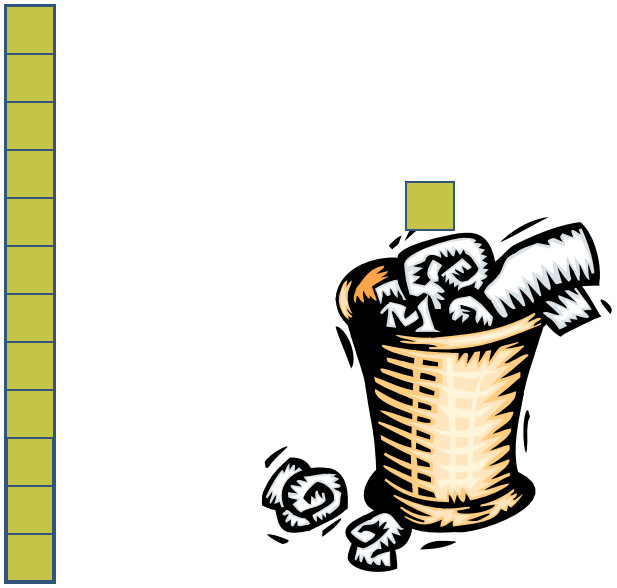
Overflow initiates a Source Quench

Overflow initiates a Source Quench

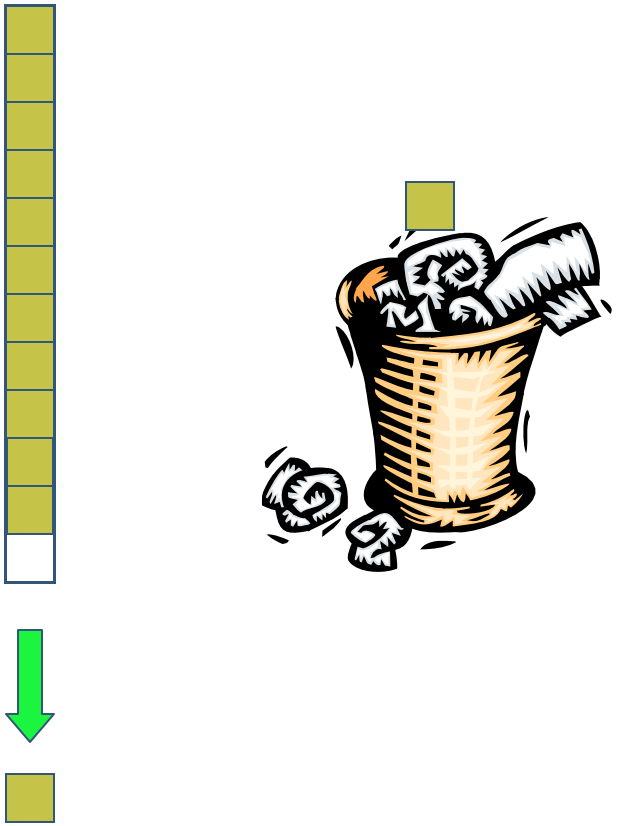
Overflow initiates a Source Quench



Overflow initiates a Source Quench

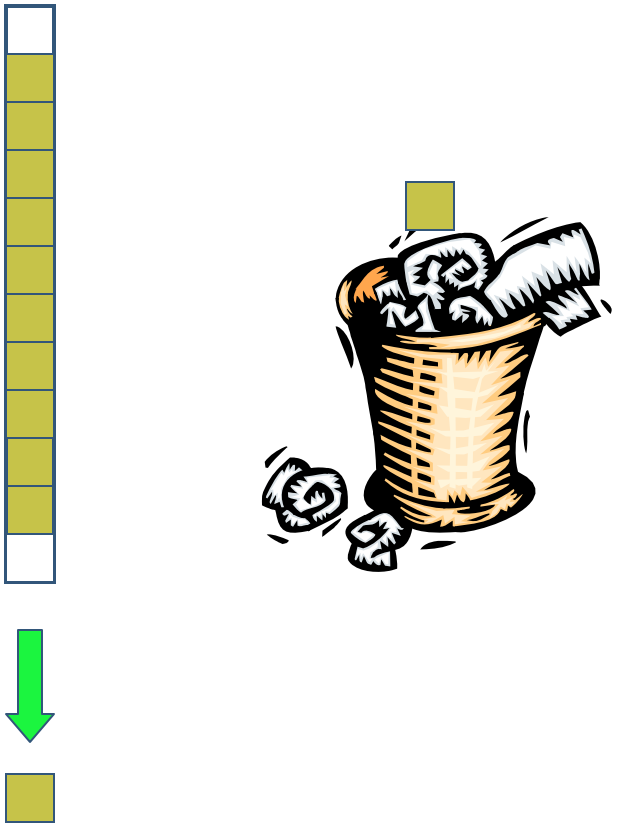


Overflow initiates a Source Quench

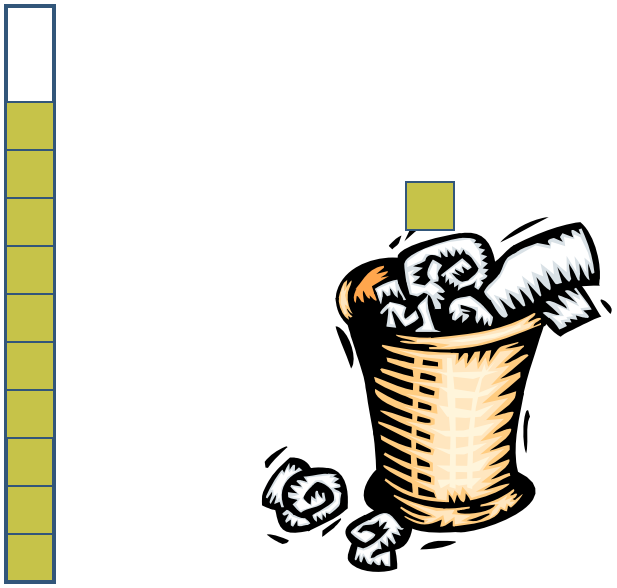


Overflow initiates a Source Quench

Overflow initiates a Source Quench

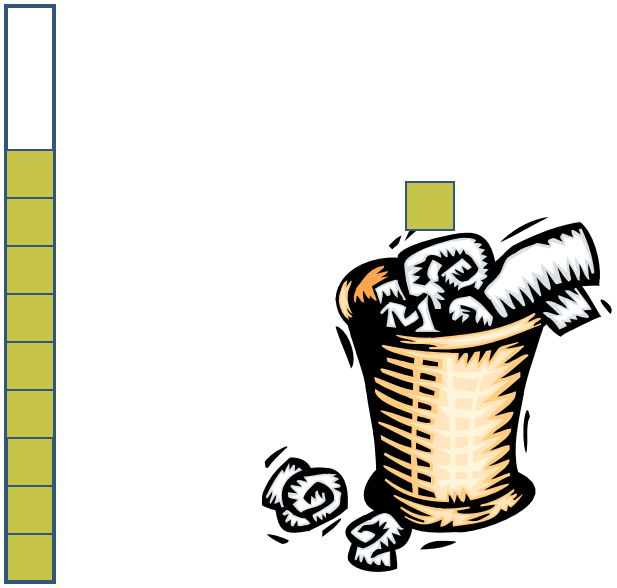


Overflow initiates a Source Quench



Overflow initiates a Source Quench

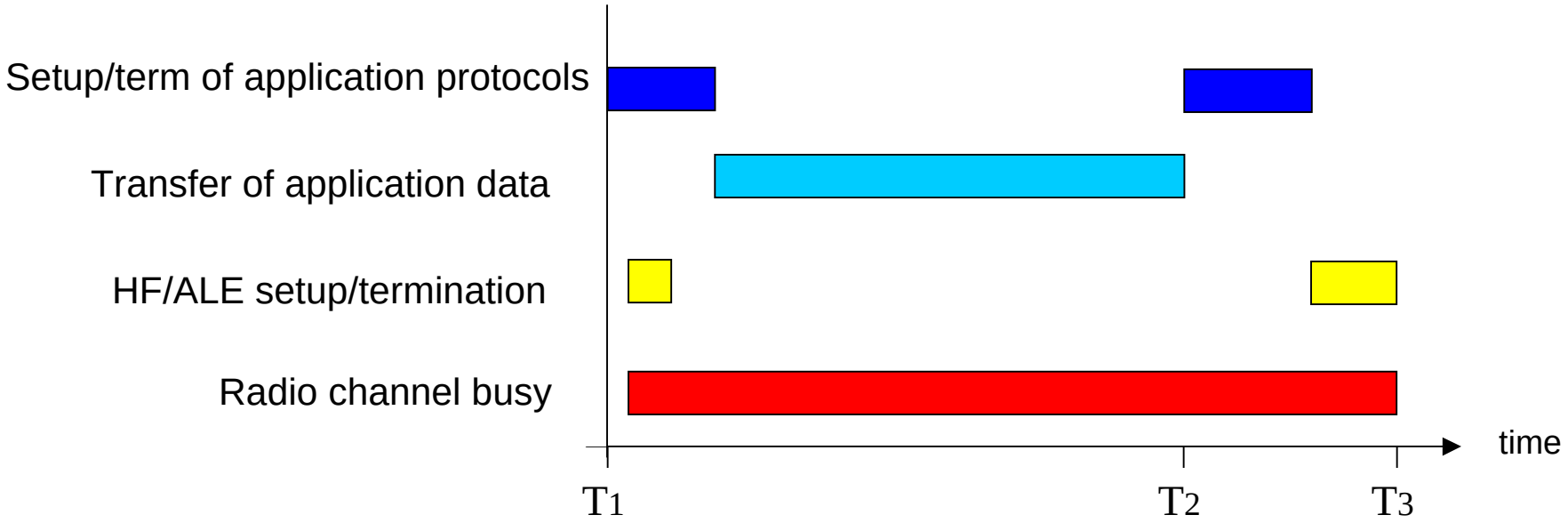
Overflow initiates a Source Quench



Congestion Control

- The HF link will inevitably represent a bottleneck in the IP network (with great impact on the quality of service being offered to the user)
- There is no flow control mechanisms defined in S4406 Annex E
- The XOmail implementation and the RF-5800H supports the use of ”Source Quench” as a local congestion control mechanism
- With some tuning of parameters, this mechanism gave acceptable performance
- Source Quench is not usable with IP crypto, and will not be supported in IP version 6
- NATO and the CCEB are suggesting an end-to-end congestion control mechanism to be included in P-Mul

Definition of Application throughput

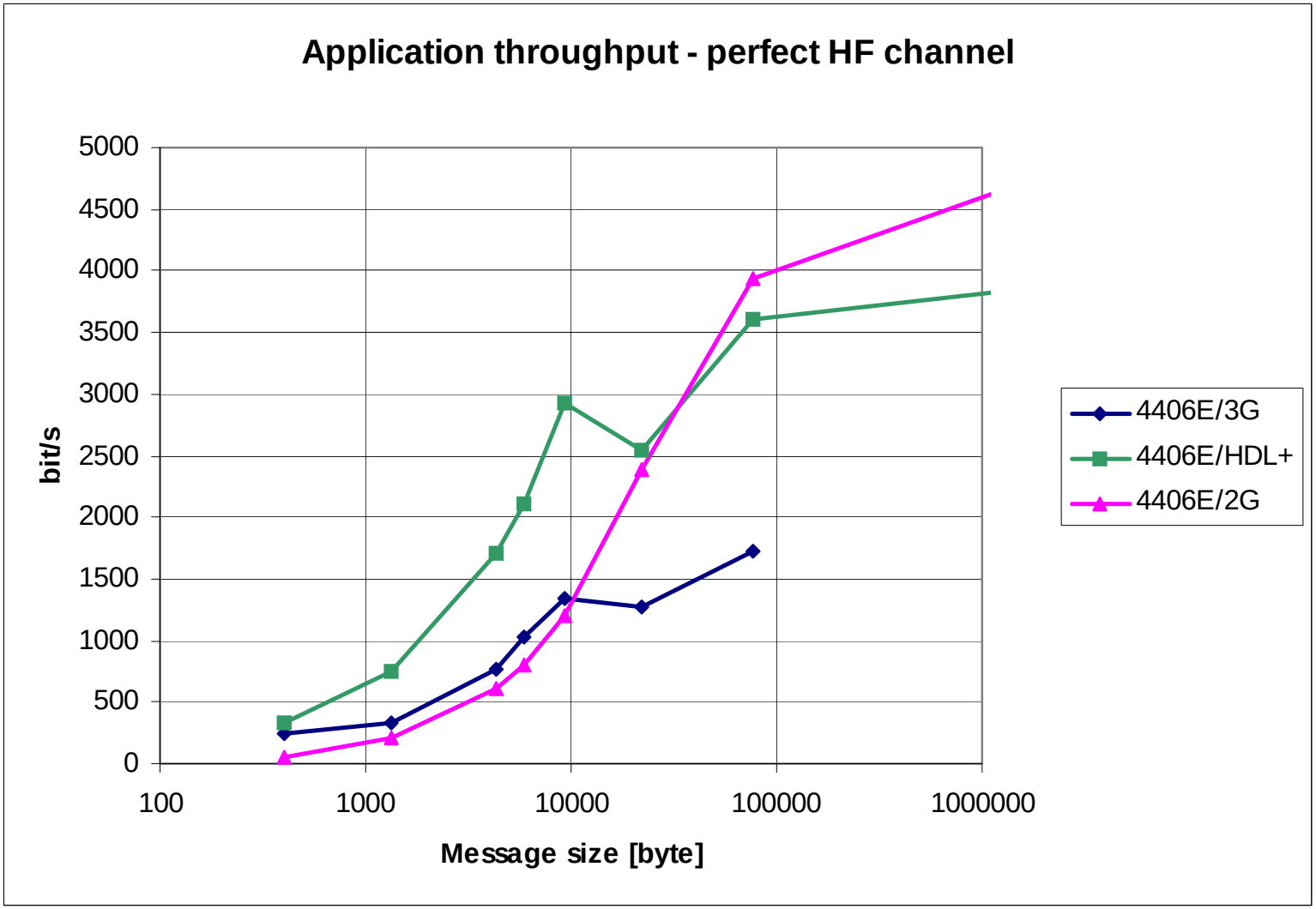


Transfer time = $T_2 - T_1$

$$\text{Application throughput} = \frac{8 \times \text{File size [byte]}}{(T_2 - T_1)[s]} \quad \text{bit/s}$$

(optimistic estimation of the HF system capacity since link termination time is not encountered, (T3 – T2))

Application throughput vs message size – ideal channel

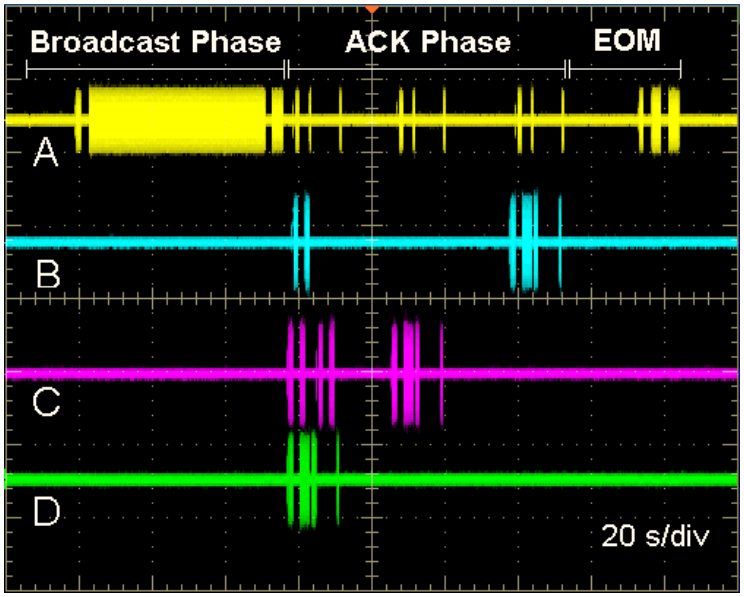


IP Multicasting over HF

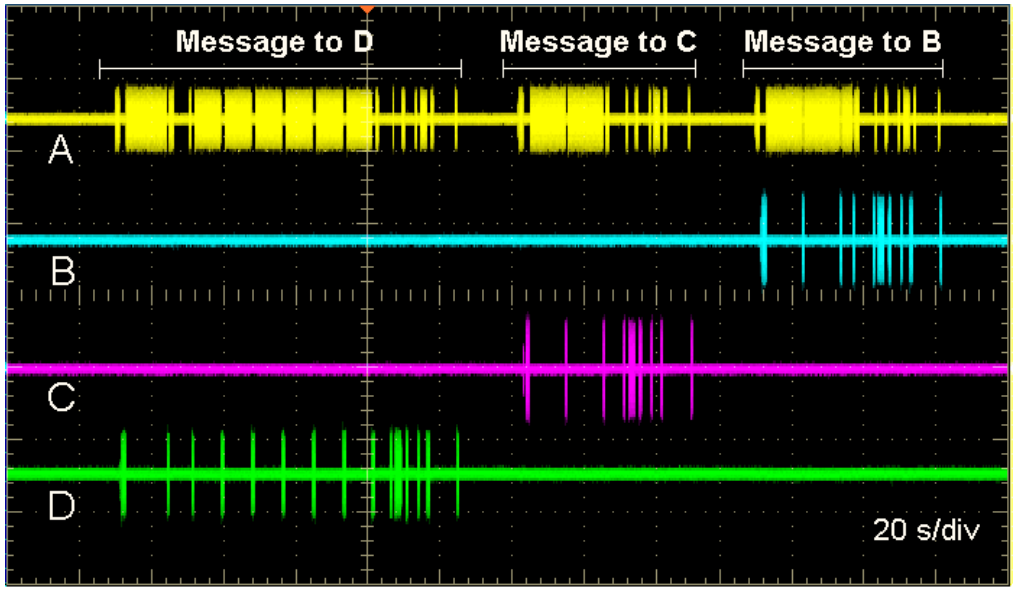
- May provide a bandwidth efficient transfer capability
- STANAG 4406 Annex E (P-Mul) provides a multicast capability
- 2G HF offers a broadcast packet service. 3G/HDL+ does not, but the RF-5800H from Harris offers an IP broadcasting service on which a limited IP multicast service can be based
- The broadcasting services of the HF systems are unreliable
- A fixed modem waveform and data rate must be chosen for the broadcast, and the probability of packet delivery depends heavily on the data rate selected
- P-Mul provides reliability of the message transfer by an ACK/NACK mechanism from each multicast recipient

Multicast vs repeated Unicast

-using the IP broadcast service of the RF-5800H



Multicast



Repeated Unicast

”A” is sending a 2.5 kbyte message to recipients ”B”, ”C”, and ”D”

SNR = 6 dB

IP broadcast data rate = 600 bps

Multicast over HF - observations

- Message delivery time is considerably shorter for the multicast message than for the repeated unicast messages
- There are collisions on the channel when all recipients are sending their message acknowledgement at the same time. However, the S4538 protocol seems to be able to resolve this channel allocation conflict, but at the cost of HF channel seizure time
- The advantages of Multicast will increase for an increasing number of recipients.
- The multicast service is stuck with the fixed data rate selected, whereas the unicast service will adapt the data rate to changing channel conditions, giving increased advantages to unicast when channel conditions are varying
- S4406 Annex E combined with an efficient multicast link protocol has the potential of providing an attractive solution to one-to-many HF communications scenarioes

”Apple and Pear comparison”

STANAG 4406 Annex E

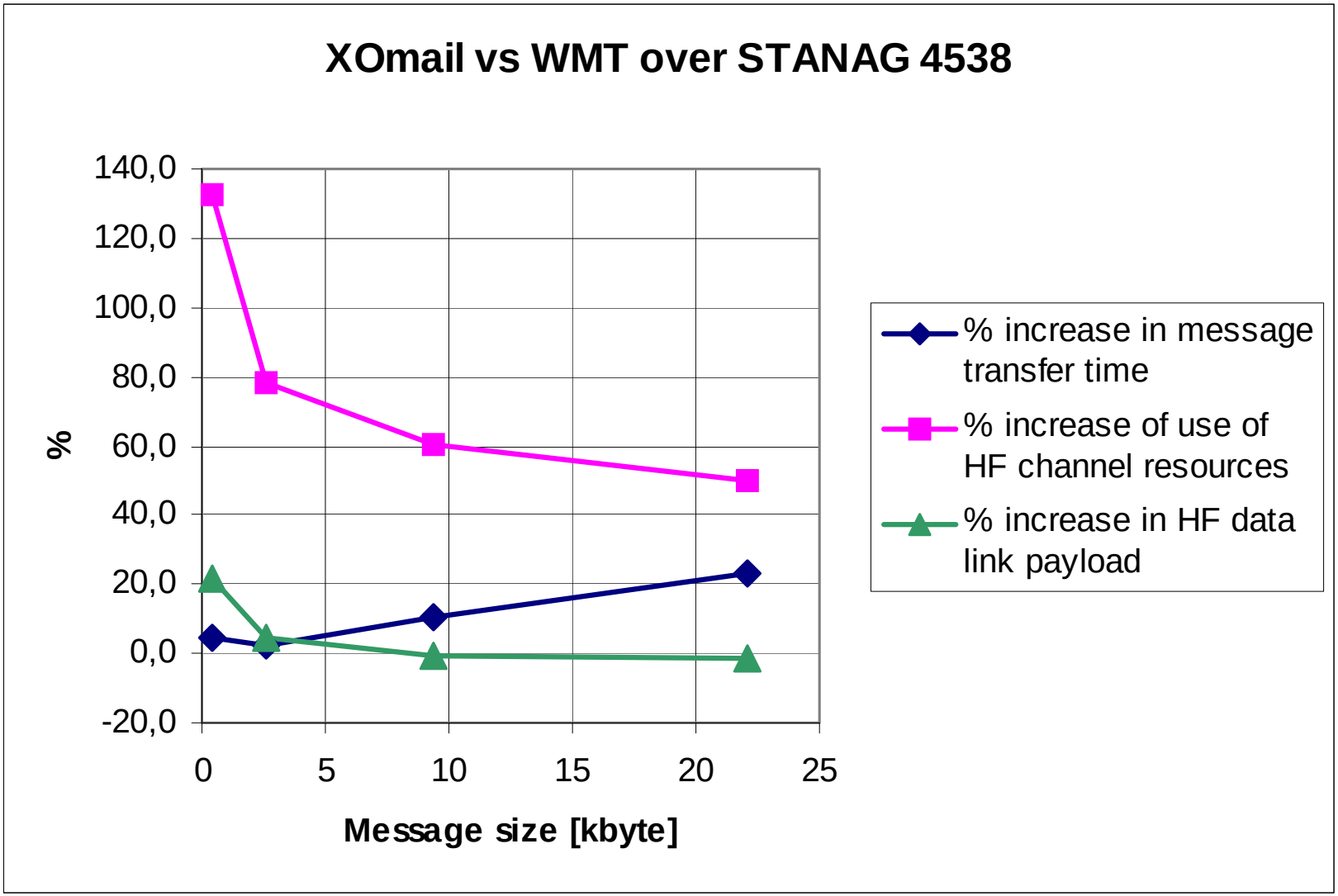
- formal messaging is a tool for military command and control
- provides seemless inter-operability with strategic MMHS

- uses a transparent IP service
- provides networking functionality enabling multiple hops
- true end-to-end acknowledge-ment securing reliability of message delivery

Dedicated HF messaging application, CFTP

- efficient packaging of messages for HF transfer
- direct mapping of the application information to the HF link layer
- provides no networking functionality
- provides no true end-to-end delivery confirmation

A comparison of XOmail vs WMT over STANAG 4538



Conclusions

- By using the STANAG 4406 Annex E protocol profile, a reliable message transfer is possible over an IP network which comprise an HF link
- S4406 Annex E over HF systems provides application throughput up to a few kbit/s
- There are optimization issues at different levels of the protocol stack, and implementation choices and parameter setting have great impact on the performance of the system
- The multicast functionality of S4406 Annex E promises to be an efficient way of delivering one-to-many traffic when used in conjunction with a suitable HF link service